Annex A: Factsheet on National Cyber Security Masterplan 2018

The infocomm security masterplans provide the strategic directions to guide Singapore's national efforts to enhance cyber security for public, private and people sectors. The first Infocomm Security Masterplan (2005-2007) initiated Singapore's coordinated approach to secure Singapore's infocomm environment with key emphasis on providing public sector with capabilities to mitigate cyber threats. In 2008, the ISMP was succeeded by the second Masterplan (2008-2012) that strove to make Singapore a 'Secure and Trusted Hub' with special attention paid on the nation's critical infocomm infrastructure (CII).

A new five-year National Cyber Security Masterplan 2018 (NCSM2018) will continue to reinforce Singapore's cyber security by intensify efforts in the Government and CII as well as the wider infocomm ecosystem which includes businesses and individuals. It is developed through a multi-agency effort led by IDA under the guidance of the National Infocomm Security Committee.

The vision of NCSM2018 is for Singapore to be a "Trusted and Robust Infocomm Hub" by 2018. It aims to engender a secure and resilient infocomm environment and a vibrant cyber security ecosystem. The three key areas of NCSM2018 are to:

1. Enhance the security and resilience of critical infocomm infrastructure
2. Increase efforts to promote the adoption of appropriate infocomm security measures among individuals and businesses
3. Grow Singapore's pool of infocomm security experts

I. Enhancing the security and resilience of critical infocomm infrastructure

Critical infocomm infrastructure

As part of the continuous efforts to enhance the protection of critical infocomm infrastructure (CII) and improve cross-sector response to mitigate widespread cyber attacks, the Government will work closely with critical sectors on cyber security exercises as well as for high priority critical infrastructure to be assessed for vulnerabilities and ensure that security capabilities and measures are in place to mitigate cyber threats.

The Critical Infocomm Infrastructure (CII) Protection Assessment programme aims to assess the security of the infocomm systems that are critical to the operation of critical infrastructures in Singapore. Building upon MP2, the Government will expand its effort and collaborate with more critical sectors to ensure high priority CII in each sector remains secure and resilient.

The National Cyber Security Exercise programme aims to enhance the readiness and responsiveness to significant cyber attacks at the national level. It will comprise of exercises that are currently conducted within critical sectors to assess the operators' capability and readiness. New cross-sectors exercises will be carried out to improve the overall resilience of our national infrastructure and services.

Government

As part of the continuous efforts to enhance the security and resilience of its infocomm infrastructure, and public sector capabilities, the Government will focus on proactive defense-in-depth to mitigate increasingly sophisticated attacks. Such attacks have made the task of threat prevention even more challenging. This includes upgrading of existing detection and analysis capabilities and strengthening preventive and recovery measures at the Whole-of-Government level.

The enhanced Cyber Watch Centre (CWC) will provide a wider range of detection capabilities for government agencies with improved correlation capabilities. Apart from continuing to provide and manage security monitoring services for the Government, supported by tested procedures and advanced monitoring technology, the enhanced CWC will leverage on more advanced tools and techniques to improve the overall security monitoring effectiveness for the public sector.

The enhanced Threat Analysis Centre (TAC) will leverage on state-of-the-art analytical tools to assess larger volume of data from a wider range of sources and to identify cyber threats with greater accuracy and efficiency. This will enable public agencies to receive detailed cyber threat analysis, threat advisories and recommendations and take preventive actions in a timely manner.

II. Increase efforts to promote the adoption of appropriate infocomm security measures among users and businesses

Current efforts will be reinforced to raise infocomm security awareness and adoption amongst users and businesses. This includes the Cyber Security Awareness and Outreach programme to augment existing outreach channels (e.g. via online and social media platforms, educational talks, road-shows, seminars, and print advertorials) and explore new avenues that offers wider coverage and reach to users, such as broadcast media.

The NCSM2018 will also include efforts to facilitate information sharing between the Government and private sector, as well as collaborate with industry and trade association to promote cyber security and exchange of threat information.

III. Grow Singapore's pool of infocomm security experts

The threat posed by rising cyber attack sophistication is exacerbated by the shortage of cyber security experts needed to counter them. A stronger presence of cyber security professionals in Singapore will help generate greater interest and a more vibrant ecosystem for cyber security expertise here. This will put Singapore in a better stead to defend against sophisticated cyber threats and to retain cyber security talent given the global shortage and high demand for them.

The NCSM2018 will look into developing human and intellectual capital within the infocomm industry to boost cyber security in Singapore. This will involve working with Institutes of Higher Learning to incorporate cyber security into their curriculum or explore the provision of specialist track in the current degree programmes. For security professionals, the NCSM 2018 will foster the development of cyber training facilities for testing and training of cyber security experts. There are also plans to promote R&D thereby attracting and cultivating more cyber security expertise.